Cyber Strike Solutions, LLC

Cyber Security reborn. Rising above.

Point of contact: Dr. Jeffrey Struik, CISSP, CASP+, Pentest+
Phone Number: (319)512-3195
Contract number: 47QTCA20D00B8

SIN Number: 54151HACS
Description: Highly Adaptive Cyber Security Services
SIN Number: 54151S
Description: IT Services

2939 170th St.
South Amana, IA 52334
319.512.3195
www.cyberstrikesolutions.com

Cyber Strike Solutions, LLC

Cyber Security reborn. Rising above.

Table of Contents

2939 170th St.
South Amana, IA 52334 319.512.3195 www.cyberstrikesolutions.com

Cyber Strike Solutions, LLC

Cyber Security reborn. Rising above.

Who We Are

Cyber Strike Solutions, LLC (CSS) was founded May 2018 in Eastern Iowa. We started because of our passion for cyber security and protecting our customers from cyber-attacks. We believe in providing exceptional technical expertise where there is no compromise in the quality of security while achieving the required performance and usability. Our expertise spans traditional IT systems, building automation/SCADA, embedded systems, tactical systems, and beyond. The Available Services section describes the various services provided by CSS.

Terms and Conditions

SCOPE

a. The prices, terms and conditions stated under Special Item Numbers 54151HACS and 54151S exclusively to Cyber Security (CS) and Information Technology (IT) Professional Services within the scope of this Multiple Award Schedule.
b. CSS shall provide services at CSS's facility and/or at the ordering activity location, as agreed to by CSS and the ordering activity.

ORDER

a. Agencies may use written orders, blanket purchase agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made, and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003). Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.
b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

PERFORMANCE OF SERVICES

a. CSS shall commence performance of services on the date agreed to by CSS and the ordering activity.
b. CSS agrees to render services only during normal working hours, unless otherwise agreed to by CSS and the ordering activity.
c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
d. Any CSS travel required in the performance of CS/IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all CSS travel.

STOP-WORK ORDER

a. The Contracting Officer may, at any time, by written order to CSS, require CSS to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to CSS, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, CSS shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to CSS, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either- (1) Cancel the stop-work order; or (2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.
b. If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, CSS shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if- (1) The stop-work order results in an increase in the time required for, or in CSS's cost properly allocable to, the performance of any part of this contract; and (2) CSS asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the

Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.
c. If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.
d. If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

RESPONSIBILITIES OF CSS

CSS shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Dec 2007) Rights in Data – General, may apply.

RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to security regulations, the ordering activity shall permit CSS access to all facilities necessary to perform the requisite IT/IAM Professional Services.

INDEPENDENT CSS

All CS/IT Professional Services performed by CSS under the terms of this contract shall be as an independent CSS, and not as an agent or employee of the ordering activity.

ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions. “CSS” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract. “CSS and its affiliates” and “CSS or its affiliates” refers to CSS, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving CSS, any entity into or with which CSS subsequently merges or affiliates, or any other successor or assignee of CSS. An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by

CSS and its affiliates, may either (i) result in an unfair competitive advantage to CSS or its affiliates or (ii) impair CSS's or its affiliates' objectivity in performing contract work.
b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on CSS, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrict ions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

INVOICES

CSS, upon completion of the work ordered, shall submit invoices for CS/IT Professional services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

PAYMENTS

a. For firm-fixed price orders the ordering activity shall pay CSS, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to labor-hour orders placed under this contract.
52.216-31(Feb 2007) Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition. As prescribed in 16.601(e)(3), insert the following provision:
a. The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.
b. The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate

for each labor category applies to labor performed by— (1) The offeror; (2) Subcontractors; and/or (3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

RESUMES

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

APPROVAL OF SUBCONTRACTS

The ordering activity may require that CSS receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

DESCRIPTION OF IT/IAMPROFESSIONAL SERVICES AND PRICING

a. CSS shall provide a description of each type of CS/IT Service offered under Special Item Numbers 54151HACS and 54151S and will be presented in the same manner as CSS sells to its commercial and other ordering activity customers. If CSS is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.
b. Pricing for all CS/IT Professional Services shall be in accordance with CSS's customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience and minimum education.

Cyber Strike Solutions, LLC

Cyber Security reborn. Rising above.

HACS Labor Categories

LABOR CATEGORY	LABOR DESCRIPTION	LABOR PRICE (INCLUDING IFF)
PRINCIPAL CYBER SECURITY ENGINEER	Analyzes and defines security requirement for computer systems which may include mainframes, workstations, and personal computers. Designs, develops, engineers, and implements solutions that meet security requirements. Provides integration and implementation of the computer system security solution. Provides oversight and guidance to the cyber security team.	$220.31 per hour
SR. CYBER SECURITY ENGINEER	Analyzes and defines security requirement for computer systems which may include mainframes, workstations, and personal computers. Designs, develops, engineers, and implements solutions that meet security requirements. Provides integration and implementation of the computer system security solution.	$164.06 per hour
CYBER SECURITY ENGINEER	Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Designs, develops, engineers, and implements solutions that meet network security requirements. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle	$126.56 per hour
JR. CYBER SECURITY ENGINEER	Works under the guidance of a Sr. Cyber Security Engineer conducting the following: Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Designs, develops, engineers, and implements solutions that meet network security requirements. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle	$85.28 per hour
SR. CYBER PROGRAM MANAGER	Manages long-term IT engineering projects. Performs engineering design evaluations and works to complete projects within budget and scheduling restraints. Develops, implements, and monitors information systems policies and controls to ensure data accuracy, security, and regulatory compliance. Reviews reports of computer and peripheral equipment production, malfunction, and maintenance to determine and address problems.	$126.56 per hour
CYBER PROGRAM ANALYST	Monitors CSS/subcontractors performance for compliance with the terms and conditions of the initial Statement of Work and to all other contractual obligations. Generates/reviews contract modifications when/if required and prepares all invoices and associated documentation for Government submittal. Supports the Program Manager and the Business Manager.	$71.81 per hour

2939 170th St.
South Amana, IA 52334 319.512.3195 www.cyberstrikesolutions.com

Cyber Strike Solutions, LLC

Cyber Security reborn. Rising above.

IT Labor Categories

LABOR CATEGORY	LABOR DESCRIPTION	LABOR PRICE
PRINCIPAL IT ANALYST	Provides extremely high-level subject matter proficiency for work described in the task. Provides advanced technical knowledge and analysis of highly specialized applications and operational environment, high-level functional systems analysis, design, integration, documentation, training, and implementation advice on complex problems that require doctorate level knowledge of the subject matter for effective implementation.	$164.06 per hour
SR. IT ANALYST	Performs a variety of systems engineering tasks and activities that are broad in nature and are concerned with major systems design, integration, and implementation, including personnel, hardware, software, budgetary, and support facilities and/or equipment. Provides quality assurance review and the evaluation of new and existing software products.	$126.56 per hour
IT ANALYST	Analyzes and develops computer software possessing a wide range of capabilities, including numerous engineering, business, and records management functions. Develops plans for IT systems from project inception to conclusion. Analyzes the problem and the information to be processed. Defines the problem and develops system requirements and program specifications, from which programmers prepare detailed flow charts, programs, and tests. Coordinates closely with programmers to ensure proper implementation of program and system specifications. In conjunction with functional users, develops system alternative solutions.	$94.75 per hour
JR. IT ANALYST	Analyzes information requirements. Analytically and systematically evaluates problems of workflows, organization, and planning and assists Senior Computer Systems Analyst and Computer Systems Analyst in developing appropriate corrective action. Helps develop plans for automated information systems from project inception to conclusion. Defines the problem and develops system requirements and program specifications, from which programmers prepare detailed flow charts, programs, and tests. Under the supervision of a Senior Computer Systems Analyst or a Computer Systems Analyst, coordinates closely. with programmers to ensure the proper implementation of program and system specifications. In conjunction with functional users, develops system alternative solutions.	$66.33 per hour
SR. IT PROGRAM MANAGER	Leads team on large projects or significant segment of large complex projects. Analyzes new and complex project related problems and creates innovative solutions involving finance, scheduling, technology, methodology, tools, and solution components.	$126.56 per hour

2939 170th St.
South Amana, IA 52334 319.512.3195 www.cyberstrikesolutions.com

Cyber Strike Solutions, LLC

Cyber Security reborn. Rising above.

IT PROGRAM ANALYST	Monitors CSS/subcontractors performance for compliance with the terms and conditions of the initial Statement of Work and to all other contractual obligations. Generates/reviews contract modifications when/if required and prepares all invoices and associated documentation for Government submittal. Supports the Program Manager and the Business Manager.	$70.31 per hour

Available Services

Vulnerability Assessments

A vulnerability assessment conducts a thorough review of the internal components of your network. Think of it like someone inspecting the interior of your house and not simply looking at it from the outside. A vulnerability assessment looks at the internal components of your network such as routers, switches, printers/multi-purpose devices, desktop/laptop computers, and servers. This allows you, the asset owner, to see the areas where you have thorough security in place and those areas that may need a little extra attention.

The vulnerability assessment includes:

- Looking at the configuration of these devices to ensure a secure configuration is in use.
- Check the software, firmware, and operating systems to ensure that all applicable security patches are applied.
- Review of the administrative policies and procedures used to protect the overall Information Technology (IT) infrastructure.

These activities allow the IT system owner(s) to understand potential areas of weakness that could cause a larger risk to the confidentiality, availability, and integrity of internal data, or customer information.

As part of the vulnerability assessment, CSS will provide a detailed report providing an explanation of the vulnerabilities, and what types of risk it may pose to the network. It will also provide recommendations for remediation of the vulnerabilities and quantify the decreased risk through execution of the remediation. Finally, if the organization would benefit from the addition of another security service or feature, CSS will provide the recommendation along with the potential costs of incorporating the service or feature.

Cyber Strike Solutions, LLC

Cyber Security reborn. Rising above.

Penetration Testing

There are two different penetration test scenarios that CSS uses. The first is a penetration test where the only knowledge of the system we have is of the external IP addresses. This type of test involves looking at the target system as a hacker would look at the system. Black-box testing involves a great deal of reconnaissance to determine what information can be collected that would allow for us to gain unauthorized access into the network. Other techniques used during the test are:

- social engineering
- exploit development
- exploit execution

The social engineering uses tactics such as phishing emails, spoofed webpages, and even observation of employees in an attempt to gain access to the organization, either physically, or through a set of captured credentials.

The exploit development and execution are the final phases of testing. This takes the information gained from the reconnaissance and attempts to create a script or program that can gain unauthorized access to the network. If network access is achieved, privilege escalation is the next goal, to demonstrate the ability of a malicious outsider to gain access to sensitive organizational data and exfiltrate the data.

The second type of penetration test is an insider threat scenario. This test emulates the effects of an employee that is attempting to gain unauthorized access to organizational information assets. During this test, CSS will use social engineering techniques and other tools to escalate privileges and gain unauthorized access.

After the penetration test is complete, CSS provides a detailed report. This report includes explanation of how unauthorized access was achieved along with the data that was accessed or exfiltrated. Further, it will share techniques to remediate the exploitable vulnerabilities, including technical and administrative remediation.

Secure System Configuration

CSS provides secure system configuration. There are many different organizations providing technical guidance for securing the systems within the network boundary. CSS will:

- Analyze the organization's regulatory requirements
- Determine how the technical security guidance applies to the organization's systems.
- Following the analysis, the technical protective mechanisms will be implemented incrementally.
- After each iteration the system will be tested to ensure proper function is still achieved.

In the event that a technical control causes malfunction, an appropriate non-technical control will be recommended, and the organization can decide if the control will meet their needs. The goal of secure system configuration is achieving maximum security with minimal impact on functionality.

Security Engineering

CSS possesses a significant amount of experience in security engineering. Our security engineering services include embedded systems, enterprise systems, and stand-alone systems. As part of the security engineering we review the design of the solution to determine what security implementations would apply to the product or system being designed. This would include conducting a comparative analysis of any available options in the security implementation to ensure that the additional security meets the customer's needs and is complementary to the system or product design. The ultimate goal of security engineering is to mitigate any potential disruptions to the product or system regardless of the origins. This means that as part of the engineering process we will take a meticulous look at any sources of disruptions ranging from malicious attacks to natural disasters and help determine how best to mitigate the risk.

Secure Architecture Design

The secure architecture design possesses similarities to the security engineering. Unlike security engineering, secure architecture design takes a broader look at the system instead of looking at components or subsystems. The secure architecture design helps provide a defense in depth approach to security. It allows for implementation of security at multiple layers within the overarching system to prevent unauthorized activities or access. CSS will take a look at the larger system and determine what security controls should be implemented to properly protect the system. The secure architecture design may include recommendations for additional policies or procedures as part of the overall risk mitigation approach. The combination of the technical and non-technical controls is designed to provide complementary overlap of

protection through the management of human factors along with the technical aspects of securing the system architecture.

Security Awareness Training

CSS realizes the importance of properly training the individuals using the information systems. Security Awareness Training focuses on the human factor of cybersecurity. We continually review current training methods and approaches to determine the most effective method of training individuals. Additionally, there is continuous updating of the training materials to address current threats, along with specific risks or threats facing a specific geographical location or industry. The intention of the security awareness training service is to mitigate as much of the risk to the information system at the user level. Methods of determining training needs include social engineering activities such as sending test phishing emails to see how many employees click the link or divulge sensitive information. These activities may also include observation of employee behaviors to see if there are any risks that may be exploited using human factors instead of technical exploitation techniques.

DoD RMF Support

CSS supports the entire Department of Defense (DoD) Risk Management Framework (RMF) process including technical control design and implementation and assistance with developing the necessary policy documents. We understand the importance of achieving system authorization as soon as possible and support our customers in achieving authorization. Our understanding of the National Institute of Standards and Technology (NIST) 800 series Special Publications (SP) enables us to provide accurate and efficient support to our customers navigating the RMF Assessment and Authorization (A&A) process.